12-2017

A Comparative Analysis of Forensic Methods Used on a Microsoft Surface Book

Michael Graham
Purdue University

A COMPARATIVE ANALYSIS OF FORENSIC METHODS USED ON A MICROSOFT SURFACE BOOK COMPUTER

by

Michael Graham

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer and Information Technology

West Lafayette, Indiana

December 2017

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF THESIS APPROVAL

Dr. Marcus Rogers, Chair
Department of Computer and Information Technology
Prof. Anthony Smith
Department of Computer and Information Technology
Dr. Baijian Yang
Department of Computer and Information Technology

Approved by:
Dr. Eric T. Matson
Head of the Graduate Program

ACKNOWLEDGMENTS

I would like to extend a huge thank my wife my parents and my extended family for supporting me throughout this long endeavor. Their love and encouraging words have helped me push through the tough times and tough assignments.

TABLE OF CONTENTS

LIST OF TABLES vi
LIST OF FIGURES vii
DEFINITIONS viii
ABSTRACT x
1. INTRODUCTION 1
1.1. Statement of the Problem 1
1.2. Significance of the Problem 2
1.3. Statement of the Purpose 2
1.4. Assumptions 3
1.5. Delimitations 3
1.6. Limitations 4
1.7. Summary 4
2. REVIEW OF THE LITERATURE 5
2.1. What is Digital Forensics? 5
2.2. Forensic Method 6
2.3. Forensically Sound Techniques 7
2.4. Hard Drive Technology 8
2.5. Imaging 9
2.6. Types of Acquisitions 10
2.7. Write Blockers 12
2.8. Imaging Software 13
2.8.1. Commercial Tools 13
2.8.2. Open Source Tools 14
3. METHODOLOGY 15
3.1. Configuring the Computer 15
3.2. Gathering Forensics Image 16
3.3. Analyzing the Images 19
4. RESULTS 21

4.1. FTK Imager 21
4.1.1. Live Acquisition 21
4.1.2. Dead Acquisition 22
4.2. DD Command 24
4.2.1. Live Acquisition 24
4.2.2. Dead Acquisition 25
4.3. Paladin 26
4.3.1. Live Acquisition 26
4.3.2. Dead Acquisition 26
4.4. Autopsy 27
5. DISCUSSION 28
5.1. Recommendations 31
5.2. Summary 32
APPENDIX A. LIST OF POPULATED FILES 34
APPENDIX B: ACQUSITION RESULTS 49
REFERENCES 55

LIST OF TABLES

Table 1 Imaging Software..17

LIST OF FIGURES

Figure 1 Workstation Setup 17
Figure 2 FTK Bash Script 23
Figure 3 Batch File 24
Figure 4 DD Bash Script 25
Figure 5 WinHex Results 30
Figure 6 BitLocker Volume Header 31

DEFINITIONS

This section describes a few of the terms used throughout this study that are not necessarily defined elsewhere.

Basic Input-Output System (BIOS): Information of the computer hardware system and serves as the intermediary between the hardware and the operating system software of the computer system (Bonomo et al., 2003).

DD Command: A simple UNIX mechanism used to extract information (Movall, Nelson, & Wetzstein, 2005).

Dead Forensics: Take place after an incident was detected and confirmed (Grobler, Louwrens, & Solms, 2010a).

Digital Forensics: The analysis of digital evidence which includes network forensics, computer forensics, mobile device forensics and malware forensics (Casey, 2011).

Forensic Image: Will contain current files as well as slack space and unallocated space (Vandeven, 2014).

Gigabyte: A measure of storage capacity equal to 1024 megabytes or 1,073,741,824 bytes (Merrian-Webster, 2017a).

Hardware Write Blocker: a hardware device that attaches to a computer system with the primary purpose of intercepting and preventing (or 'blocking') any modifying command operation from ever reaching the storage device (NIST, 2004).

Live Forensics: Gathering of live evidence during an ongoing attack (Grobler, Louwrens, & Solms, 2010b).

Logical Image: Analysis involving using the native operating system, on the evidence disk for a forensic duplicate, to pursue the data (Easttom, 2014).

MD5 Hash: Algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input (Rivest, 1992).

Physical Image: Offline analysis conducted on an evidence disk or forensic duplicate after booting from a CD or another system (Easttom, 2014).

Software Write Blocker: Tool that protect drive access through the interrupt 0x13 BIOS interface of a PC (NIST, 2003).

Solid-state Drive (SSD): A nonvolatile memory chip using Negated AND gate-based flash memory, which retains memory even without power (Easttom, 2014).

Terabyte: 1024 gigabytes or 1,099,511,627,776 bytes (Merrian-Webster, 2017b).

Ultrabook: A high-end subnotebook defined by Intel (Intel Corporation, 2012).

ABSTRACT

Author: Graham, Michael M.S.
Institution: Purdue University
Degree Received: December 2017
Title: A Comparative Analysis of Forensic Methods Used on a Microsoft Surface Book. Major Committee Chair: Dr. Marcus Rogers

The research question being asked by this project is which tool is the most effective at dead forensics and which is the most effective at live forensics when working on time-sensitive cases that involve a Microsoft Surface Book? The Microsoft Surface series of products is an example of one of the new products containing a non-removable solid-state storage drive. These laptop computers are becoming very popular and offer something that most other tablets do not, a full size USB port capable of transferring data on and off the device. This port can allow connectivity of many different device and most simultaneously with the help of a hub. This port can finally allow investigators access to the internal storage of the device. Many techniques were attempted in order to recover data, however due to time constraints this project only tested a few open source techniques along with some commercially developed software. This project examined multiple tools, along with the knowledge and resources needed to perform data recovery. It was found that the Microsoft Surface Book has some form of encryption being utilized at all times even if the user has not enabled BitLocker. The only way this project was able to successfully recover data from the computer was by utilizing FTK Imager on a live system while logged into a profile. This new knowledge will help digital investigators to more effectively gather data both on-scene and in a lab environment.

1. INTRODUCTION

1.1. Statement of the Problem

Forensic practices began back in the 1100s. Digital forensics, in relation, has only been studied since the 1980s (Garfinkel, 2010). The field of digital forensics is a relatively new field of study when compared to the other forensics disciplines. This field is also evolving at a blistering pace (Carnegie Mellon University, 2017) It started as computer forensics but soon expanded to include all types of digital technology. New types of devices are created every year with different features and different operating systems. Digital investigators have a strong need to discover ways to obtain forensic images of the newest devices available. Some of the newer devices are tablets and Ultrabook computers (Shim, 2012). These often feature a touchscreen with no keyboard, mouse, or removable storage. These devices are typically very thin and light. In order to accomplish this small footprint, manufacturers have done away with the standard mechanical storage disks with rotating magnetic media and replaced it with ultra-fast solid-state drives that plug directly into or are soldered onto the motherboard.

Devices with solid-state storage soldered directly to the motherboard pose a potential problem for investigators. Some forensic practices would prefer the hard drive to be removed from the suspect computer when possible and connected to the examination computer through a write blocker to prevent potentially changing any data on the suspect drive (SWGDE, 2014). This is simply not possible with the new type of storage. Investigators need to find a way to access a system and image the storage without being able to physically remove the drive.

1.2. Significance of the Problem

This research is important to the digital forensic community because there is a growing need to obtain vital information as quickly as possible, especially when on a scene of a time sensitive investigation (Rogers, Goldman, Mislan, Wedge, & Debrota, 2006). Critical information can be found on various electronic devices retrieved from suspects or even good Samaritans willing to help. This information could help investigators find violent criminals, the possible location of a terroristic act being planned, or possibly the whereabouts of a child that was abducted from their parents.

Mobile computing is a market many users have decided to step into and purchase a tablet/detachable to replace the traditional computer in their homes. Vendors that have traditionally been a leader in the laptop market have decided to expand their product lines to include the detachable (2-in-1) devices consumers have been clamoring for (Eddy, 2016). As demand for these devices continues to rise, investigators will have to learn how to quickly obtain information pertinent to an investigation. The research for this thesis set out to discover the method(s) which can gather all of the sought after data on a computer in order for a digital investigator to quickly image and search the internal SSD of a detachable computing device in order to find the critical information needed.

Methods discovered during this research can be adapted to existing forensic methods. Future computers may contain internal storage, which could be soldered directly to the motherboard and cannot be removed without damaging other components.

1.3. Statement of the Purpose

The goal of this research was to determine which forensic tool is the most effective at dead forensics and which is the most effective at live forensics when working on time-sensitive cases that involve a Microsoft Surface Book. For the purposes of this research, the most “effective” method is determined by which tool can recover most/all of the sought after data coupled in the shortest amount of time. Multiple tools were examined along with different techniques. The tools were graded based on their speed as well as accuracy. In the field of forensics, a higher emphasis must be on evidential integrity and security. It is for this reason the results were graded as follows, a single point for every second it took to acquire the image. An additional 5 points will be added for every artifact missed or with mismatched hash values. The points for each tool were be added up and the lowest score was determined to the be the most effective. The results of these experiments were used to answer the research question, “Which forensic technique is best suited for a Microsoft Surface Book in a time sensitive investigation?”

1.4. Assumptions

There are several assumptions made when designing the methods used in this analysis:

- Investigations can benefit from digital evidence immediately found on-scene
- The software write blocking capabilities are working correct to prevent data from being changed
- All extractions are performed using forensically sound techniques
- All ports on the suspect laptop are intact and working to their full capabilities

1.5. Delimitations

The delimitations of this study include:

- Time does not allow all possible extraction software to be tested
- Performance of external hard drives may vary
- Not all known file types were placed onto the computer for extraction

- Only the USB 3.0 interface is available for data transfer

1.6. Limitations

The limitations of this study include:

- This study only examined speed and accuracy
- This study only tested and compared three imaging tools
- This study only uses a single Microsoft Surface Book

1.7. Summary

This section was written with the intent to shed light on this research project including the scope, significance, limitations, delimitations, and assumptions. The purpose of this research is to find the most effective way for cyber investigators to obtain information from the Microsoft Surface Book computers that feature non-removable storage drives. This is a problem that most investigators will soon face if they have not already. The hope was to identify a specific tool and/or technique, which enables the investigator to quickly and accurately find important evidence during a time-sensitive investigation.

2. REVIEW OF THE LITERATURE

The review of literature performed for this research identified a lack of knowledge as it pertains to imaging newer style computers without removable media. These types of devices present new challenges to analysts as they become more and more popular and therefore are more likely to hold a key piece of evidence during an investigation. It was the purpose of this research to determine which tools, and techniques are best in time-sensitive situations. The differences between tools could translate into valuable information being located in a shorter time.

2.1. What is Digital Forensics?

Forensic practices have occurred starting back in the 1100s. Digital forensics, in relation, has only been studied since the 1980s. The field started as computer forensics only but soon expanded to include all types of digital technology. Advances in technology have led to greater data storage capacity, along with a significant increase in the number of devices each person owns (Waring, 2014). The increased reliance on electronic devices might also be a contributing factor to a soaring jump in cybercrimes. Criminals could use digital devices to send threatening emails, fraudulently transfer money, harass others or conduct other illegal businesses (Lessard & Kessler, 2010). Digital forensics is a division of the forensic community that focuses on the digital world as a whole. Not only do these investigators perform analysis on home computers, but also mobile devices, network forensics and even corporate security. Digital evidence is present in most investigations even if the user(s) are unaware of it (Årnes, 2017). Computers can be the target of a crime, an instrument used in the commission of a crime, or simply a place where relevant evidence might be stored (Easttom, 2014). This makes the job of digital investigators a difficult one to say the least.

2.2. Forensic Method

When conducting an investigation on digital devices, it is paramount that one performs every task with a purpose and documents what they do and why they do it. The Digital Forensic Research Workshop (DFRWS) has put together a framework for how a digital investigation should be conducted (Tahiri, 2016). There are six individual levels to the investigation process:

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation

These levels lay the groundwork for a solid investigation that could be used during a criminal investigation. The identification phase of an investigation is used to determine what devices are relevant evidence in the case being pursued. For example, an inkjet printer may not be considered relevant evidence in a network hacking case. The lead investigator will later determine the relevance. Once relevant devices have been determined, it is best practice to do everything possible to preserve the evidence in the manner it was found so as not to potentially disturb any evidence that might be present within the device. Mobile phones that are found powered on should be left on but isolated from the network (SWGDE, 2013). The collection phase of an investigation consists of gathering devices from the scene. Each device should be photographed in its original position and secured in a manner that follows accepted procedures. Next is the examination phase, which consists of an in-depth search of the evidence to locate primary and even secondary evidence that may be hidden on a device. Primary evidence would consist of actual files that are being sought after (Casey & Schatz, 2011). Additional evidence might consist of the metadata relating to the primary evidence. This could mean a forensic image for computers and physical, logical, and/or file system extractions for cell phones. This gathering is done in such a way that the evidence is disturbed the least amount possible to limit any changes that may occur to relevant data (Årnes, 2017). The analysis phase of the investigation will not only look at the evidence collected but what these files mean (Al-Fedaghi & Al-Babtain, 2012). Recording the times files were created or when they may have last been accessed is vital to creating a timeline of the events that took place. Modified, accessed, created (MAC) timestamps can be used to identify a timeline of events that happened relating to the event in question (Casey, 2011). The presentation phase is used to present all the evidence in layperson's terms to an authoritative figure such as judge or jury. The presentation should include a summary of all the evidence and explanation of conclusions that were drawn from the evidence.

2.3. Forensically Sound Techniques

The techniques used by examiners need to follow a set of guidelines established by the forensic community to ensure data is being collected in a manner which maintains its integrity. The growing use of digital forensics in the court system has pushed for the development of forensic processes (Mckemmish, 2008). Multiple subject-matter experts as well as local, state, and federal law enforcement agencies review many of these guidelines.

This research used practices recognized by the digital forensic community as being forensically sound. Ensuring digital evidence is collected in a forensically sound manner is key to ensuring the results are consistent and fair. An example of best practice techniques can be found in the a pocket guide for first responders (Department of Homeland Security & United States Secret Service, 2007). The disk imaging tools used in this study have been verified by the NIST

Computer Forensics Tool Testing Program (CFTT) (NIST, 2017). Each case for investigators feature unique scenarios and challenges that need to be documented and overcame. All of these documents are used to provide the examiner with guidance on the best way to obtain and secure digital evidence (Judish, Hagen, Bailie, & Jarrett, 2009).

2.4. Hard Drive Technology

Standard mechanical hard drives have been around for many years. The inner workings consist of rotating platters which contain data, a read/write head, and a circuit board. These pieces work together to store data on this nonvolatile media. The platters are coated with a thin layer of metal which can be magnetized or demagnetized to hold data. As the platters spin around, the read/write head seeks the desired information on the platters. Depending on how fast the platters are spinning and how spread out the data is, this could be seen as slowness to the user (Vamsee, 2011).

An SSD is also nonvolatile store media but uses different technology than the standard hard drive. Unlike the hard disk drive, SSDs contain no moving parts. These drives are made up of NAND flash memory modules and a controller (Micheloni, Marelli, & Eshghi, 2013). Data is stored on these modules and is constantly moved around to keep files are contiguous as possible. The ability to move data at faster speeds gives these drives an incredible performance advantage (Benusa, Jeganathan, & Schmidt, 2016). A SSD also uses much less power than a standard hard drive which is ideal for laptop users seeking an extended battery life.

2.5. Imaging

When digital evidence is obtained, it is considered best practice to create a duplicate of the original media and then perform an analysis from the copy (Department of Homeland Security & United States Secret Service, 2007). Leaving the original intact will ensure its integrity as well as allow other copies to be made if needed. The copying of the data bit-by-bit is called a forensic image and includes all slack/unallocated space (Vandeven, 2014). A forensic image is a type of duplication generally performed using a hardware or software write-blocker which prevents the original data from being changed in any way. These images can be either a physical image that captures every single bit of information on a disk or a logical image that will capture only the active data on the machine. This will be discussed in the next section.

In the early days of digital forensics, tape drives and hard drives were a type of nonvolatile storage that used magnetic media to storage bits of information. Mechanical hard drives feature multiple spinning magnetic platters to hold data. A read/write head will search each platter as it spins in order to deliver the data to the user. Current hard drive sizes can be as large as twelve Terabytes for 3.5” versions (Western Digital, 2017) and five Terabytes for 2.5” versions (Seagate, 2017). Solid-State Drives (SSDs) use flash memory chips to store data. These chips allow for SSDs to come in a various form factors and range in capacity from two Gigabytes on up to 60 Terabytes (Paulsen, 2016).

Digital forensic methods first relied on booting to a preinstallation environment to image a hard drive in a forensically sound manner (Pollitt, 2010). In more recent years, as technology has allowed for the widespread use of SSDs in computers. The compact size has allowed manufacturers to develop laptops that are lighter and thinner than ever before. The new designs of laptop make it very difficult to remove the storage media, and some might even be soldered onto the motherboard. Physically dismantling these types of laptops is a time consuming endeavor which could risk damaging the storage device and potentially destroying the data stored within it. SSDs do have a unique property that investigators must fight against. A program in the firmware of most SSDs will cause data to be written evenly over the entirety of the disk. This means that some data may potentially be moved around to fill up unallocated space whenever power is applied to the drive. This technique is referred to as wear-leveling and can cause data to be erased and those blocks re-written almost immediately (Kumar & Vijayaraghavan, 2015).

2.6. Types of Acquisitions

Before starting the imaging process of storage media, it is best for the examiner to determine what type of image will be most valuable for the current situation. A physical image is one that captures every single bit of information contained on a drive including all of free and wiped space. This process is much more thorough and generally takes much longer. A logical image only captures the user data that one would see during normal use of the computer (Kemmerich et al., 2014). When performing a logical acquisition on a computer system, the tool does not seek to capture deleted and unallocated spaces of the drive. This can sometimes result in a faster acquisition, however; it is less thorough than the physical image. A live data acquisition is used on systems that are currently running and stays running while the image is taken. This data includes RAM, currently running processes as well as information on the hard drive (SWGDE, 2014b). Lastly, a Targeted file acquisition is one where specific files are requested along with related files such as LNK files, registry keys, and Jump lists (SWGDE, 2014)

The logical image may be the preferred imaging technique if investigators are working on a time sensitive case. This method will allow investigators to view the easily accessible information which may result in a great lead in the investigation. The downside to this method is that hidden data won't be discovered until a more thorough acquisition can be completed in a laboratory. In these cases, the on-scene examiner might choose to follow the Cyber Forensic Field Triage Process Model which focuses on finding the vital information in a short period of time (Rogers et al., 2006). The potentially shorter processing time of a logical image can make a significant difference in an investigation.

Another decision that needs to be made at the scene of an investigation is whether or not live or dead recovery will be used. A live forensic image is obtained while the machine remains powered on. This might be suitable for machines suspected to contain full disk encryption (Brian Carrier, 2005). A portion of live forensic process also includes gather the information currently residing in the computer's memory. This is known as a RAM Dump. This type of acquisition will seek to extract data from system memory, currently running processes, networking, registry, and even malware (Gohel & Upadhyay, 2017). Dead forensic recovery requires that all processes be terminated and the machine be powered down (Bell & Boddington, 2010). If the storage device is removable, it is then plugged into a write blocker so the data cannot be overwritten.

Finally, once the forensic image is complete, cryptographic hash values are calculated called MD5 and SHA-256. These hash values are critical to forensic examiners because it helps them to determine if the copy that was obtained is exactly the same as the original. If even a single bit of a file is changed, it will result in a completely different hash value being calculated (Kornblum, 2006). These hash values also help the examiner differentiate between known operating system files and files created by the user. MD5 hashes will look at all the information being process and run it through an algorithm producing a 128-bit value. A SHA-256 hash performs the same procedure but with a different algorithm producing a 256-bit value.

2.7. Write Blockers

Write blockers are a set of devices that have been used for many years in the digital forensic community. The primary goal of a write blocker is to prevent any data on the source drive from accidentally being changed during the imaging process (Lyle, 2006). It is imperative the data is not changed during the investigative process even a little bit. The court must feel confident the investigator used sound forensic technique and the processes used must pass the Daubert Standard (Easttom, 2014). Even the slightest bit of doubt can render the digital evidence inadmissible (Goodison, Davis, & Jackson, 2015).

There are two types of write blocker commonly used during investigations. The first is a software write blocker that uses special software installed on the examination machine. The software will only allow certain ports on the machine to act in a read-only mode. It does this by preventing write commands from making it to the disk controller. Specifically, this method uses the INT13 interrupt at the BIOS level to interpret read/write instructions. The write blocker will determine if certain commands from an application are allowed or blocked (NIST, 2003). Based on the result, either the command will be sent to the disk for execution or it will fail immediately so no more changes can be made to the disk. Most software write blockers can be turned off which will allow full functionality to return to all ports on a computer. They can also be prone to failure due to a myriad of reasons. Since the write-blocking procedure relies on the host hardware, software updates can create compatibility issues. Motherboard and other hardware failures can result in a failure to interrupt commands (Menz & Bress, 2004).

A hardware write blocker performs the same functions as a software write blocker however; the write blocking software interacts directly with the application layer and the controller while the hardware write blocker is a physical piece of equipment that is attached between the storage media and the examiner’s computer. It is important that the device has the most up-to-date firmware to be compatible with a wide-range of devices. The write blocker will then look at commands being send to the suspect storage media and prevent modification requests from reaching the drive controller (NIST, 2004). These write blockers can be portable so they can be used at the scene of an incident. Portable write blockers can be manufactured to be read-only while some can be manufactured to be read/write devices (Tableau, 2017).

2.8. Imaging Software

There are multiple tools that investigators use to image computers. Some of these tools are commercially made while others are open source. The commercially made tools are created by for-profit companies which have a vested interest in creating products able to perform above and beyond others on the market. Open source tools are those created as a collaboration between many programmers whom work on the source code to improve from its original design (St.Amant & Still, 2007). The collaborators typically check each other’s work to ensure there are minimal flaws.

2.8.1. Commercial Tools

Forensic Toolkit (FTK) is a commercially built product from AccessData used to create images and analyze data found on computers. FTK also includes a standalone utility for imaging media called FTK Imager. This software can be ran from within an operating system or on a flash drive (FTK Image Lite) (Bone, 2016). FTK has been used by many computer forensic professionals and cited in many journal articles and court cases for many years. It has also been tested by the Department of Homeland Security using the Computer Forensics Tool Testing (CFTT) program (Department of Homeland Security, 2016). This software has been shown to be a vital piece of software for digital investigations.

2.8.2. Open Source Tools

Paladin is a free Linux software based on the widely popular Ubuntu. Paladin was created by Sumuri and features over 100 built-in tools to assist with investigations. Autopsy started life in 2001 as a GUI to TCT and TCTUTILs. A complete rewrite of this system in 2008 has turned it into what is now seen today (Carrier, 2017). This distribution contains many free forensic tools built in to help perform both simple and complex tasks even if network connectivity is not available.

The DD command is one of the oldest digital forensic imaging tools still in use today. This command is built into the GNU Coreutils package which has been built into Linux, Mac OS X, and even Windows. It is a command line application that uses several controls and switches to control exactly how an image of the machine is captured.

The research performed describes a gap in the current knowledge as it pertains to this computer. The Microsoft Surface Book is a 2-in-1 computer quickly becoming popular with consumers featuring a non-removable solid-state drive. Research into forensic techniques for this computer is sparse. This research devised a plan to close the gap in knowledge by using the tools described above on both a live and a dead system to find which tool can quickly acquire data. These devices are becoming more and more mainstream, and this will likely be involved in future cases that investigators encounter. The results of this research will guide on-scene investigators to choose which tool will work best for them based on the computers discovered during the search as well as the state of those computers. Choosing the correct tool will help to expedite the search for valuable data.

3. METHODOLOGY

The goal of this research is to determine which tool is the most effect at dead forensics and which is the most effective at live forensics when working on time-sensitive cases that involve a Microsoft Surface Book. The research is broken into four different steps to accomplish this task.

1. The first step was to start with a computer that has a fresh installation of Windows 10. This was done to delete any previous data so as not to taint the results of the acquisitions.
2. Next, the computer was populated with data that might be found on an everyday home-use computer.
3. The next step was to complete both live and dead forensic acquisition using the tools described later. A live acquisition sought to gather all the data a dead acquisition would gather along with all currently running processes, open files and any other data residing in RAM. The tools were measured by their speed and consistency of data acquisition.
4. Finally, the measured data was analyzed to determine how the tools performed in time-sensitive situations.

3.1. Configuring the Computer

First, the Microsoft Surface Book needed to be setup with a clean image downloaded directly from Microsoft and pre-populated with data. The pre-population of data will help to determine the accuracy of the different imaging software being used. To start, a suitable computer for this research is a Microsoft Surface Book with an Intel Core i5-6300U 2.40GHz CPU, 256GB SSD and 8GB of RAM. The Surface Book received a complete erase and reimage with Windows 10 Professional 64-bit Creators Update. After the reimage process was complete, a local user account named “Criminal” was created. This account is the sole administrator account. A second, standard, user account “Son” was also created for more data to be populated. Both accounts have a separate and unique password. This sought to see if there was a different between administrator and standard user accounts. Next, all current patches and updates were installed.

After the test profiles were created, they were populated with the files found in the Appendix A. The data populated in both accounts were mostly downloaded from various sources on the internet, some files were manually created. The data consisted of MP3 files, PDF documents, Word documents, images, videos, and html links as these are some of the most popular file types found on a consumer’s computer (Garfinkel, 2007). After the Surface Book setup was complete, the user data was populated by creating word documents, downloading MP3, MP4 and image files from multiple sources on the internet. Also, PDF files were copied to the machine from a flash drive. Once all data was populated, the storage location of the data was noted. In addition, an MD5 hash was calculated for each individual file as well as the overall system so this could be compared to the hashes of the files and image captured during the subsequent acquisitions.

3.2. Gathering Forensics Image

Ten total acquisitions were ran for each tool as well as for each method to establish a reliable baseline for length of time needed for each acquisition. All ten acquisitions were compared to each other for consistency. This will provide an accurate average for how each tool performs under the given circumstances. Due to these computers having non-removable storage, the hard drive could not be removed and the imaging software must use the Surface Book’s hardware to run. The imaging software was delivered via USB 3.0 thumb drive to maximize speed. The imaging software being tested in this research was chosen due to their popularity and vetting from the Department of Homeland Security.

Table 1 Imaging Software

Tool	Version
FTK Live Imager	3.4.3.3
Paladin	7.0.2
Autopsy	4.4.0
DD	7.2.641

These tools were used to conduct both live and dead forensics. The live forensics were conducted with the computer turned on and logged into the administrator account.

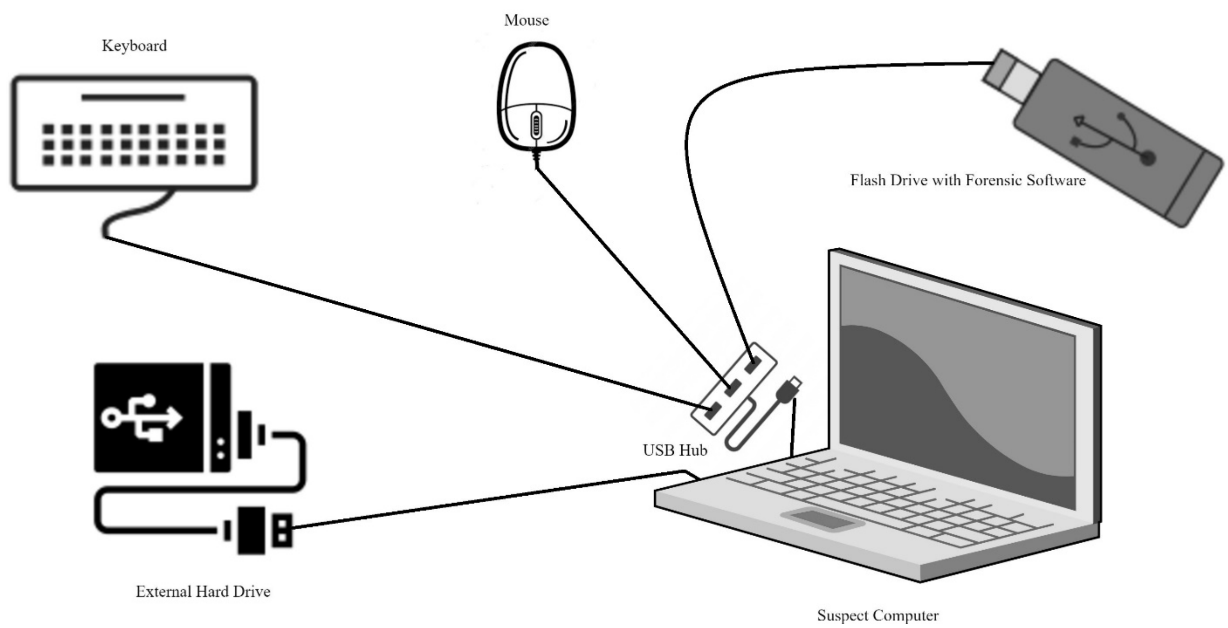

Figure 1 Workstation Setup

The equipment was setup as seen in Figure 1 above. The researcher could now begin the actual imaging of the machine. Due to the unavailability of drivers within the Linux kernel, a USB hub had to be utilized for the keyboard to work properly. This was done based on initial observations while attempting to perform dead acquisitions using the Paladin boot drive.

To obtain a "forensically sound" image of the suspect drive it is best to follow the steps laid out by the Scientific Working Group of Digital Forensics (SWGDE, 2014).

Step 1: The forensic software was loaded onto a 64GB USB 3.0 flash drive. The external keyboard, mouse and flash drive were plugged into one of the USB ports on the left side of the computer using a USB hub.

Step 2: For the dead forensic scenarios, the computer needed to boot from the USB flash drive. To boot to the flash drive on a Surface Book the researcher must hold the volume-down button, followed by a press and release of the power button.

Step 3: The image being created was added to an 8 terabyte external hard drive that is connected to the other USB 3.0 port to maximize speed.

One may notice there is no hardware write blocker being used in this process, this is because the storage media cannot be physically removed from the device. A hardware based write-blocker is used for just that, preventing write commands. In this scenario, a write command is necessary from the USB stick to run the forensic software. While the forensic software is running, it will need to be able to write to the external hard drive used to the capture the acquisition. In these cases, a software write blocker is implemented to prevent any unauthorized changes from taking place on the suspect system. During the imaging process, a time will be kept to determine how long each tool took to complete the imaging task.

The process described above was used to acquire images using the software in table 1. First was FTK Live Imager on a live system followed by the DD command. The remaining tools were not designed to be used on a live system therefore the researcher was unable to test them at this point. Once complete, the computer was shut off and booted to the flash drive containing a bootable image of Paladin. From this flash drive, Paladin, FTK Imager, and the DD command were able to be ran. After further inspection of the Autopsy software, it was determined this software used the DD command to perform imaging. Since this process was already tested there was no need to re-test. The start and end times of each acquisition were also recorded for later comparison.

3.3. Analyzing the Images

The images obtained throughout the processes described above were analyzed and compared in speed and accuracy to determine which software/process is best for certain situations. Each image was processed using FTK Toolkit. FTK examined the images and laid out the file system in use along with all the user data collected within its respected location. First the images were divided into a “Dead” or “Live” category based on the status of the system when the image was obtained. As explained earlier, a dead system is one that is powered off and booted to the forensic software to create the image while a live system is one that is already powered on and the image much be created without shutting the system down for fear of losing any data. All data within the “Dead” category was compared against all other data in that same category. The same was done for the “Live” category.

Within each category, the number of artifacts collected was compared to the original artifacts to ensure all possible data was captured. The images were also analyzed for the length of time it took to obtain the image. The size of the image was taken into consideration when determining the amount of time. Lastly, the times from the dead acquisitions were compared against each other and the times from live acquisitions were compared against each other.

Another way these images were analyzed is how well each tool was at recovering some/all of the data populated on the computer. After the data was first placed on the computer, an MD5 hash was calculated and recorded into a chart. Each tool was repeated ten times on a live machine and ten times on a dead machine. There was a total of 50 acquisitions obtained for this research.

The hash values for the complete images were also recorded. The data populated onto the machine was attempted to be located and a hash of that file was recorded and compared to the original hash value obtained earlier. Any change in the hash values may indicate the data was modified in some way or only partially captured. The way in which the data was changed might not be obvious or relevant.

This process continued for all artifacts placed on the machine using both sets of images from each technique. The hashes were placed into a table for easy comparison to determine which, if any, files were modified between being placed on the machine and the first image, or between the first image and the second image.

Once all the data was collected and analyzed, the hope was to have a clear distinction between the different tools and techniques being used. Perhaps there are situations that a certain tool with a certain technique is better than others. The data also told us if data is changed during the imaging process with these new computers. A modification of the data would need to be accounted for when presenting the finding to a court of law.

4. RESULTS

The test profiles were created on the computer according to the procedures outlined in the methodology section. The results of the testing procedures are grouped by the test cases. The live acquisitions were chosen to be ran first. If a computer is discovered in the on state in the field, it is best to leave it turned on in accordance with SWGDE Best Practices (SWGDE, 2014). Once a computer has been turned off, it can never be returned to the state it was found. While still turned on, the computer was examined and data was collected using the tools described above.

4.1. FTK Imager

4.1.1. Live Acquisition

FTK Imager Lite was downloaded and placed onto the 64GB USB 3.0 flash drive. An MD5 hash was taken of the flash drive before any acquisitions took place. The computer was then logged into using the known password. The program was executed and a logical acquisition was performed of the OS partition. The data was captured on a Western Digital 8TB external hard drive. As explained earlier, each acquisition was ran ten times to obtain an adequate sample of the performance from each tool.

The results of the ten acquisitions showed that FTK Imager Lite took an average of 2,850 seconds or 47 minutes and 30 seconds to complete each acquisition. All acquisitions were exactly 244,191 MBs in size. The average speed of this tool was 89.2MB/s. A table with all data can be found in Appendix B.

Once all acquisitions were complete, they were added into FTK Toolkit to be processed as evidence. Analyzing of each acquisition took place using FTK Toolkit v5.3.3.9. FTK was able to locate all of the populated data in the location it was placed as shown in Appendix A. MD5 hash values calculated by FTK were exact matches to the MD5 hashes calculated before all acquisitions were started. The length of the file, in bytes, was also a match to the original state. The overall MD5 hash of the separate images were all unique with no repeats. This suggests the TRIM feature is working and changing operating system files, but not the user data files that were populated onto the device. Lastly, an MD5 has was taken of the flash drive afterwards to ensure no new data had been placed on the flash drive. The hash file matched the original value showing that no data on the flash drive was changed during the acquisition.

4.1.2. Dead Acquisition

The dead acquisition was performed using FTK Imager Command Line for Linux. This was downloaded onto a flash drive that contained a bootable image of Paladin. A bash script was created that would output the start time of the acquisition, then use OS partition at the input and output the resulting image to the external hard drive as an e01 file. Lastly the finish time of the acquisition was output in the terminal screen. This script was repeated ten times in a row using a For loop.

```
#!/bin/bash

INPUTDEV="/dev/nvme0n1p4"

for i in {1..10}; do
   echo "-----------------------------------";
   echo "Time started: $(date)";
   echo "Running: FTKIMAGER if=$INPUTDEV
FTK_Dead_Image$i"
   time /ForensicsApps/Imaging\ Tools/ftkimager $INPUTDEV
/media/WD/FTK_Dead_Image$i --e01
   echo "Time ended: $(date)";
   echo "-----------------------------------";
done
```

Figure 2 FTK Bash Script

The results of the ten acquisitions showed and average time to complete of 3,192 seconds or 52 minutes and 12 seconds. Each acquisition was 243,631 MB in size. Average speed of the acquisition was 76.32 MB/s. A table with all data can be found in Appendix B.

Analysis of the dead FTK images was unsuccessful. FTK Toolkit was unable to process any of the ten acquisitions. All acquisitions contained an unknown file system.

4.2. DD Command

4.2.1. Live Acquisition

To obtain a live acquisition using the DD command, dc3dd was downloaded onto the flash drive and ran from a command prompt using a batch file. In the command string, E:\ referred to the flash drive and D:\ referred to the external hard drive used for data capture. This file allowed the acquisition to run ten times without interaction, with the only change being the output file name.

```
@echo off
echo %DATE%%TIME%
e:\dc3dd.exe if=\\.\PHYSICALDRIVE0 of=d:\DD_Live_Image.dd
echo %DATE%%TIME%
timeout /t 300
echo %DATE%%TIME%
e:\dc3dd.exe if=\\.\PHYSICALDRIVE0 of=d:\DD_Live_Image2.001
echo %DATE%%TIME%
…
echo %DATE%%TIME%
e:\dc3dd.exe if=\\.\PHYSICALDRIVE0 of=d:\DD_Live_Image10.001
echo %DATE%%TIME%
```

Figure 3 Batch File

The average time to acquire an image of the drive was 15,335 seconds or 4 hours 15 minutes and 35 seconds. Each acquisition was exactly 256,060 MBs in size. The average speed of creating the image was 16.70 MB/s. A table with all data can be found in Appendix B.

FTK Toolkit recognized the file system as having BitLocker encryption and asked for a security key despite not having configured BitLocker during the setup of the device. None of the images were able to be examined for artifacts.

4.2.2. Dead Acquisition

The dc3dd utility is built into the Paladin image. Similar to the FTK Dead acquisitions, a bash script was created to use a For loop to capture ten images right after one another. The script displayed the start and end time of the acquisition and copied the OS partition as a .dd file.

```
#!/bin/bash

INPUTDEV="/dev/nvme0n1p4"

for i in {1..10}; do
   echo "-----------------------------------";
   echo "Time started: $(date)";
   echo "Running: dd if=$INPUTDEV of=/mnt/DD_Dead_Image$i.dd"
   time /usr/bin/dc3dd if=$INPUTDEV of=/media/WD/DD_Dead_Image$i.dd
   echo "Time ended: $(date)";
   echo "-----------------------------------";
done
```

Figure 4 DD Bash Script

The average time to capture an image of the dead system using the DD command was 1,396 seconds or 23 minutes and 16 seconds. This was by far the fastest tool. Each acquisition was exactly the same size at 255,465 MBs. The average speed per acquisition was 183.39 MB/s. A table with all data can be found in Appendix B.

Analysis of these images was unsuccessful by FTK Toolkit, Autospy, and EnCase. None of the tools were able to read the file system present in the images. It was noted that each image did have the exact same MD5 hash.

4.3. Paladin

4.3.1. Live Acquisition

Paladin is a modified Linux distribution based off Ubuntu. It was designed to be a bootable ISO that must be initiated during the startup of a machine. This will not allow live acquisitions to occur using Paladin. If a computer is found at scene already powered on, this tool is not advised to be used.

4.3.2. Dead Acquisition

When booted to Paladin on a flash drive, the user is presented with several forensic tools. One of the tools built into this distribution is the Paladin Toolbox. This utility includes a disk manager which allows mounting partitions in read or read/write status. There is also a disk imager that allows for the imaging of partitions using different file formats.

When first performing the acquisitions, the ending file format was set to .e01. This resulted in an average time of 5,834 seconds or 1 hour and 37 minutes and 14 seconds. Each image was exactly 255,465 MBs in size. The average speed of acquisition was 43.84 MB/s. A table with all data can be found in Appendix B.

Upon seeing how long the .e01 images took, the researcher also conducted acquisitions using the DD format to determine if image creation was any faster. When using the DD format, the average time for an acquisition was 2,045 seconds or 34 minutes and 3 seconds. Each image was the exact same size as the .e01 counterpart. This made the average speed 126.25 MB/s.

During the examination of the images, it was found that FTK Toolkit could not read the images themselves and therefore was unable to process the information. The file system was unrecognized and did not show any useful information.

4.4. Autopsy

Autopsy was unable to be used at all during these experiments. After starting the experiments and performing more research it was determined that Autopsy could only be used in a bootable format. It was also found that the only way to image a drive using Autopsy was to simply use the DD command. Since this technique has already been tested, there was no need to attempt using this tool.

5. DISCUSSION

This study analyzed data collected from using different forensic tools to obtain live and dead acquisitions from a Microsoft Surface Book. It sought to determine which tool and technique would be preferred in a time sensitive investigation. The tools were judged on their speed and how accurately they recover the data placed on the machine. The tools used in the study included FTK Imager, Paladin Toolbox, Autopsy, and the Linux DD command.

Each tool was to be tested both with the computer in a live acquisition as well as a dead acquisition. The times of each acquisition was recorded and an average per tool was determined. The averages were compared to find which tool was able to successfully copy the hard drive of the Surface Book onto an external hard drive. While the computer was in a live state, only two of the tools were able to be utilized. FTK Imager and the DD command were the only tools of the four that were able to be ran on a live system. Between those two tools, FTK Imager was the quickest. FTK Imager was able to transfer at 89.2 MB/s, creating an image in 47 minutes and 30 seconds. The Linux DD command ran at a speed of 16.7 MB/s, creating an image in 4 hours 15 minutes and 35 seconds.

The analysis of the live acquisitions was done with FTK Toolkit. The images obtained via FTK Imager were processed and all files placed on the machine during setup were recovered with matching MD5 hash values. The total size of each file (in bytes) was also compared to the original file and all were a match. The comparisons were done by exporting the results into Microsoft Excel and then comparing the MD5 and size columns.

When attempting to analyze the DD live images however, FTK determined the volume was locked by BitLocker and requested a BitLocker password before being able to process the image.

Since BitLocker was never configured on this computer, the password was unknown and processing did not complete. The image was also attempted to be read by Autopsy and Encase. Both tools were unable to recognize the file system. This was leading to the belief that even though BitLocker had not been configured during the setup process, some sort of encryption was enabled on the machine.

When performing the dead forensics, all acquisitions were performed from a bootable Paladin USB drive. FTK was a command tool downloaded from AccessData's website and DD was included as part of the Ubuntu distribution in which Paladin is based on. The FTK and DD tools were each ran ten time consecutively using a bash script. This allowed for automation of these tasks. Paladin was ran manually and the output file name was changed between each acquisition. After doing some more research, it was determined that the Autopsy tool used the DD command for imaging. Since the DD tool was already being tested on its own, the researcher opted not to test this tool.

The DD command was the fastest tool when performing dead acquisitions. The average time took just over 23 minutes to capture an image of the 255GB operating system partition. This was the fastest time among all tools dead or live. One item that was noted for all dead acquisitions was the MD5 hash. The hash value for all 30 acquisitions were exact matches.

When it came time to analyze the dead acquisitions, none of them were able to be read by any of the tools. Each tool could not recognize the file system present within the images that were obtained. As this was found to be true with all of the images, they were double checked for encryption by using WinHex v19.3 to view the information contained within the file. All information in WinHex appeared to be obfuscated. This further suggests that some type of encryption was being used on the partition being imaged. Upon further searching of the images using WinHex, a volume header of “-FVE-FS-“ was discovered. This volume header is known to be used by BitLocker (Shabana Subair, Balan, Dija, & Thomas, 2014). These findings can be used to develop a process for on-scene investigators to follow when a Microsoft Surface Book is discovered.

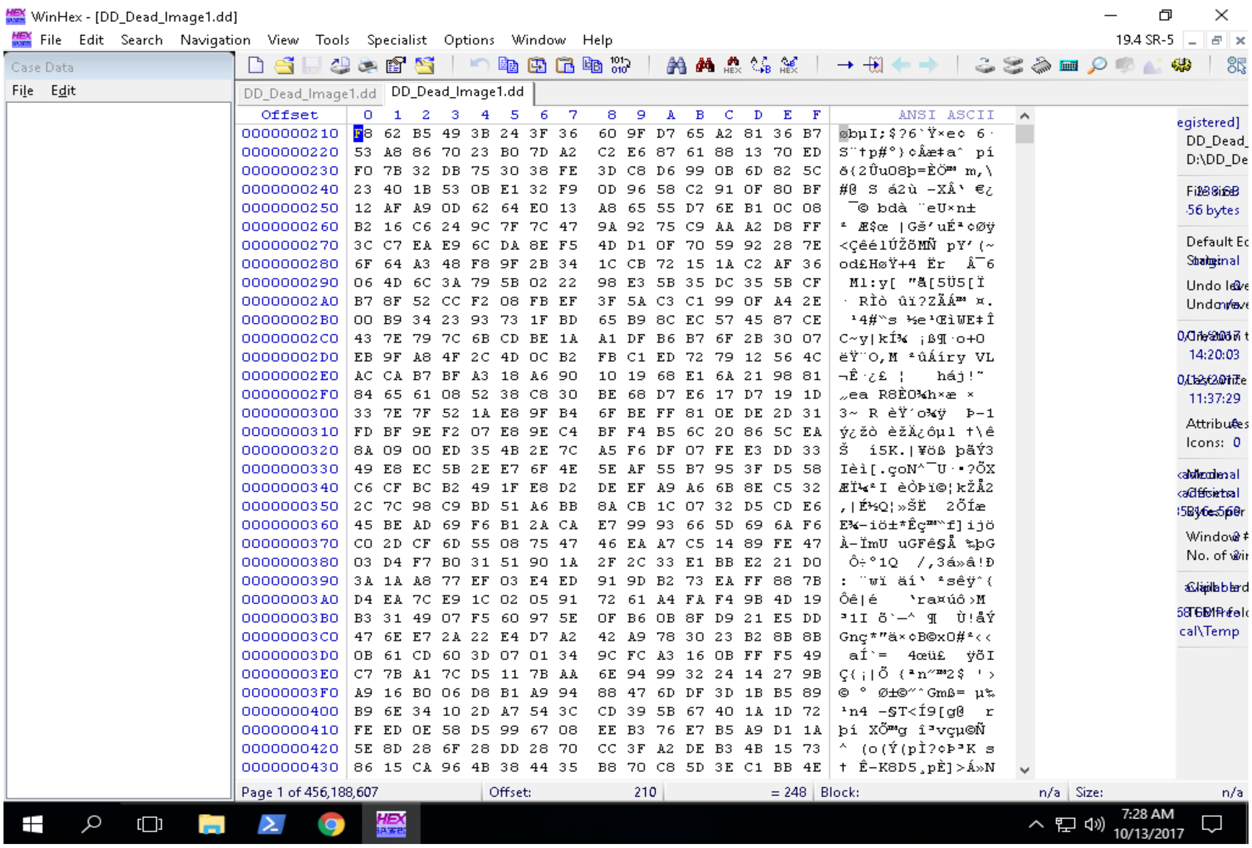

Figure 5 WinHex Results

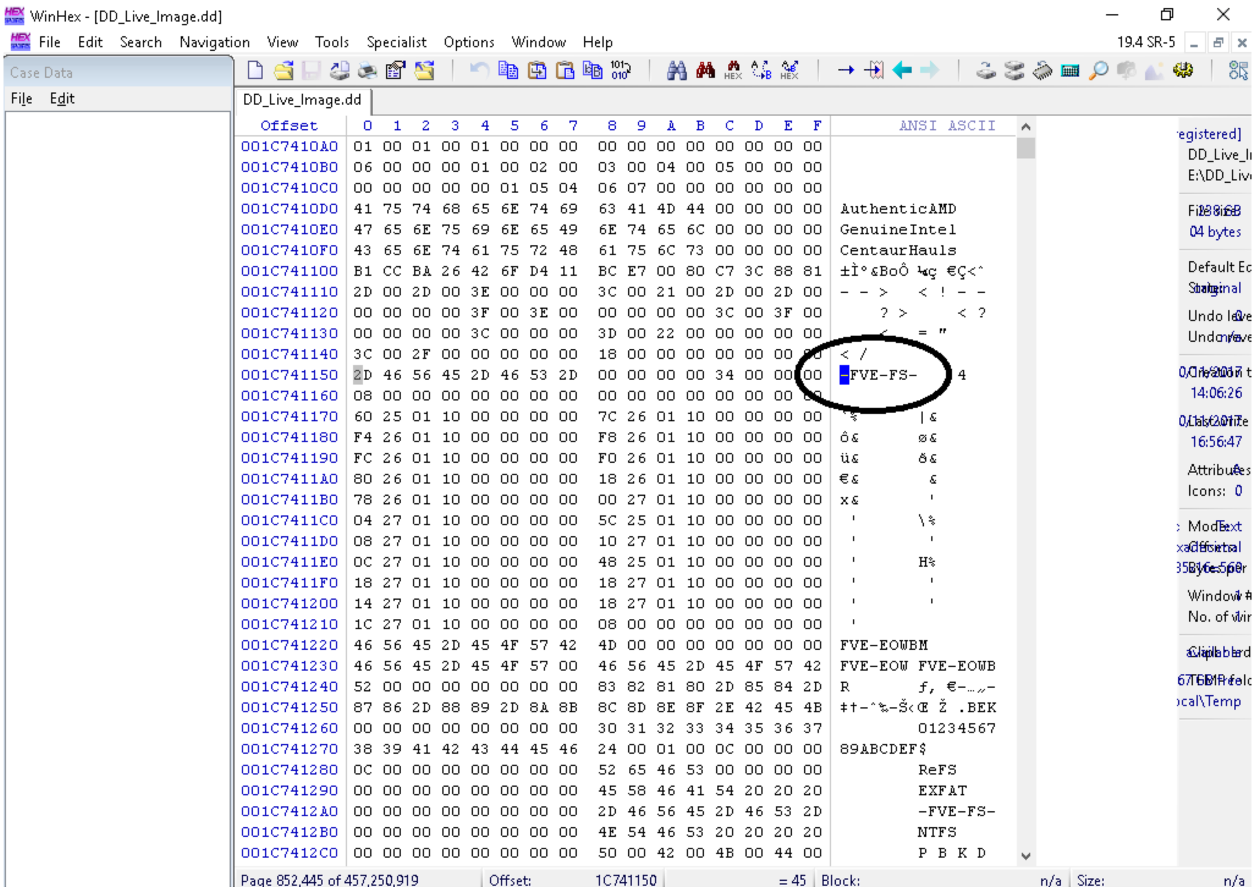

Figure 6 BitLocker Volume Header

5.1. Recommendations

The data from this study showed interesting evidence that may lead to the belief that encryption is always being used on a Surface Book without explicitly configuring BitLocker. Another aspect that could have been improved upon in this study would be keeping the operating system up-to-date. During this study, Microsoft released its Fall Creator's Update. Microsoft also recently released their second generation of Surface Book.

Another change in which could have made was using a version of Ubuntu/Paladin that has a more up-to-date kernel. The updated kernel contains the drivers necessary for the keyboard, and touchscreen of the Surface Book to work properly when booted to the Linux distribution. The ability for the keyboard to work would eliminate the need for a USB hub to be used. The USB hub could have been a source of bottleneck despite being listed as USB 3.0 speeds.

At the end of this research it is believed that encryption is always being utilized on this computer. The Trusted Platform Module (TPM) built into the Surface Book is thought to be the reason the hard drive is encrypted based on the presence of BitLocker volume headers (Arthur, Challener, & Goldman, 2015)

5.2. Summary

This study examined several tools used by the forensic community. It looked at how fast and how reliable these tools are at gathering data from a Microsoft Surface Book. These tools were attempted in both live and dead scenarios. Although not all of the tools were able to perform under both conditions, the results show that only one of the tools was able to successfully recover and process the data populated onto the machine.

Of all the tools tested, FTK Imager and the Linux DD command were the only tools that were able to be used on both live and dead machines. FTK Imager used on a live machine was the only scenario that was able to process and recover the sought after information. The remaining tools and scenarios were unable to be processed after the acquisition was complete. Based on the results of processing all the scenarios, it appears that some form of encryption is being utilized on the machine.

These findings are significant for forensic investigators. It establishes that a password is needed to gain access to the operating system in order to obtain an image of this machine. This will allow for collection of data from the machine which can be immediately examined on-scene or at a later time back at a lab. Complete disassembly of the Surface Book can be a timely endeavor and may not be practical when working on a time-sensitive case.

Future work on this topic can include using several other tools that may be better able to handle any encryption that may be in use on the machine. When using Linux as a bootable tool, ensuring the kernel is new enough to include Surface Book drivers will help to eliminate the USB hub that was utilized in this study. This researcher is interested to know if removal of the internal SSD will yield the same results as the dead acquisitions.

APPENDIX A. LIST OF POPULATED FILES

List of Populated Files

Location	File	Extension	MD5	Length (bytes)
C:\Users\Criminal\Desktop	PDF (16)	.PDF	ADF8FCC62D3212A51D9D1E14266F0A2E	33,454,054
C:\Users\Criminal\Desktop	PDF (17)	.PDF	EFB36F2C2AFB30E1B4894FCA6AF59434	15,821,086
C:\Users\Criminal\Desktop	PDF (18)	.PDF	FF67D09E8412B6A27E3C64C30D6569E2	415,683
C:\Users\Criminal\Desktop	PDF (19)	.PDF	2334F8B7F9DAA4CDAEBBC7088B43F6BF	8,441,518
C:\Users\Criminal\Desktop	PDF (20)	.PDF	7C6D6B431CC4F2CE546621E03B352447	498,340
C:\Users\Criminal\Desktop	Picture31	.JPG	98BD54A77114D4C2973EA359028F353E	96,827
C:\Users\Criminal\Desktop	Picture32	.JPG	760DD60DA0EBD1314A5448FF9F9E22E9	18,405
C:\Users\Criminal\Desktop	Pitch Perfect	.MP4	5DDF3C33CD4CB2C5B579EACEA198EDBD	1,714,599,948
C:\Users\Criminal\Documents	interm-word-newsl-calendar-trad	.DOCX	0BB85060109B48E26BC99E61F3E35EB3	13,658
C:\Users\Criminal\Documents	interm-word-newsl-calendar-yr-rnd	.DOCX	0FD1E24F07CBCB1AF3EF42843743CE3E	13,452
C:\Users\Criminal\Documents	interm-word-newsl-disclosure	.DOCX	B94A94082CE130B5EA415C154F3FE4E7	14,636
C:\Users\Criminal\Documents	MS-Word-Meeting-Itinerary-Template-Free-Download	.DOCX	AFB1BDB31955DB0C8C48CBCB634159C0	15,481
C:\Users\Criminal\Documents	PDF (1)	.PDF	02CEB6ADA35501203E611D4BA4E0718F	212,101

C:\Users\Criminal\Documents	PDF (10)	.PDF	54FA1CD7EDBA69EF45AEE2D7FD18021E	455,660
C:\Users\Criminal\Documents	PDF (11)	.PDF	2B314CC66E2204E09CDAF9DBDB10943C	3,899,645
C:\Users\Criminal\Documents	PDF (12)	.PDF	05F1EB9812A0D90DCA0FCB64D5BF535D	591,973
C:\Users\Criminal\Documents	PDF (13)	.PDF	1BDC1725F0859B866DFA5F92AA7685D5	3,209,402
C:\Users\Criminal\Documents	PDF (14)	.PDF	5CC2C55D0F2FFD40ECB23B9E12637349	244,939
C:\Users\Criminal\Documents	PDF (15)	.PDF	299365588D736FA7AAD4C60DF480DA2B	573,155
C:\Users\Criminal\Documents	PDF (2)	.PDF	497E26E6FFCB878BB6F2331632257AB0	648,048
C:\Users\Criminal\Documents	PDF (3)	.PDF	3BA6DC2B2A726C6B671ED424E688E74E	76,653
C:\Users\Criminal\Documents	PDF (4)	.PDF	C8C9E715DB9383ADBEAD4A7B38059E2C	837,584
C:\Users\Criminal\Documents	PDF (5)	.PDF	0EF8F6C564C9A78C9C02DC39DE64AB07	12,822,303
C:\Users\Criminal\Documents	PDF (6)	.PDF	4ECED06940B55F3C37E9C3387F782D60	2,585,824
C:\Users\Criminal\Documents	PDF (7)	.PDF	2FEE06D399306D6B8318DBD5DBA53489	63,168
C:\Users\Criminal\Documents	PDF (8)	.PDF	D429E97A21DEA5DFFE7218A9A1253A49	711,610
C:\Users\Criminal\Documents	PDF (9)	.PDF	5D4EE0601BBAA1543BDBF3E9F9910846	125,301
C:\Users\Criminal\Documents	Picture33	.JPG	69583BF04C9D55EAB96A56D32DF89710	147,145
C:\Users\Criminal\Documents	Picture36	.JPG	5B924174E7DE1EFE7DD0FF5BC206D069	426,491
C:\Users\Criminal\Documents	Picture37	.JPG	76DBB144DE2F07FFAE94248D5DA55CAE	219,647
C:\Users\Criminal\Documents	Resume Template - Athletic Training	.DOCX	D09BFCA8C02BDAA5A5DF504BF1065006	24,328
C:\Users\Criminal\Documents	Biology	.DOCX	1F9CEDAFCE5C38545E01FAA9B273A015	28,426
C:\Users\Criminal\Documents	Resume Template – Business_Management	.DOCX	631059213A151C4CFB86FDC153065D63	29,167
C:\Users\Criminal\Documents	Resume Template - Criminal Justice	.DOCX	AC3B4B6895869D0C17DDC3D361FBAE38	28,293

C:\Users\Criminal\Documents	Resume Template - Teaching Certificate	.DOCX	A3DF9B72704876163D2CC23DAFB5370A	28,609
C:\Users\Criminal\Documents	SampleDOCFile_1000kb	.DOC	13389334CCD51F61FC1A8296E5706D55	1,024,000
C:\Users\Criminal\Documents	SampleDOCFile_2000kb	.DOC	B74F3720A6F6A184903BC614D1A4D64C	2,048,000
C:\Users\Criminal\Documents	Schedule-of-Stay-Itinerary-Template-Free-Word	.DOC	7DA851DD6E9C86F383115458740966B7	38,912
C:\Users\Criminal\Documents	School-Itinerary-Free-MS-Word-2010-Format-Download	.DOC	7E4D8A601BA83BF68559AF05B80F3D55	145,408
C:\Users\Criminal\Documents	Study-Itinerary-Free-Word-2010-Format-Free-Template	.DOC	CD25192100AF228429E55E5F9B984874	83,456
C:\Users\Criminal\Documents	Weekly-Itinerary-Template-Free-Word-Download	.DOC	0A5E26476FE3179798329A0364D3D2E8	41,984
C:\Users\Criminal\Documents	word-course-disclosure	.DOCX	D02414087E2DF683461955BA7F8EF5CA	14,410
C:\Users\Criminal\Documents	word-interm-bowling-scores	.DOCX	2587F91B60D4B832F3AE2E24500B31E4	19,120
C:\Users\Criminal\Documents	word-interm-merging-letter	.DOCX	8415EE11CA610E88218BFA1D4E6AEFBC	11,468

C:\Users\Criminal\Documents	word-interm-newsl-hmwk	.DOCX	41A4A3152ECA69F1085B62BAAE79C976	13,708
C:\Users\Criminal\Documents	word-interm-newsl-message	.DOCX	74FE59872F20D6C141F4EDB51D6B969E	11,076
C:\Users\Criminal\Documents	word-interm-newsl-quotes	.DOCX	A3EA840D524271483394B9E610AACD45	11,281
C:\Users\Criminal\Documents	word-interm-weather-cal	.DOCX	DA6290DB72D6303EE4B7E0A8988AC1AC	58,659
C:\Users\Criminal\Downloads	Picture34	.JPG	E80B8A0E843286DEB20D270C74CEB10B	339,049
C:\Users\Criminal\Downloads	Picture35	.JPG	8AD1CF2891687EF9DFBDC5F3960A3C8A	208,803
C:\Users\Criminal\Music	01 1999	.MP3	0680A0F0415A786ECC41ABB80302DB5D	3,495,568
C:\Users\Criminal\Music	ACDC - Hell's Bell's	.MP3	A1C7F7E8F2DFFC1288732F1B516B2E63	12,554,563
C:\Users\Criminal\Music	ACDC - Highway To Hell	.MP3	FE91C03B29C3366CFE5D50BD808E337D	8,419,904
C:\Users\Criminal\Music	ACDC - T.N.T.	.MP3	43936C0A7F1C25DAD76C41DD935FF851	8,664,715
C:\Users\Criminal\Music	ACDC - You Shock Me All Night Long	.MP3	C05AB3034FE5DA4ADF46EC66A11F7875	8,496,507
C:\Users\Criminal\Music	Adele - Hello	.MP3	DEAD150EBD42788386215476C6D804BC	11,927,204
C:\Users\Criminal\Music	Air Supply - All Out of Love	.MP3	0BA83EF447157FE2678E6021E579F2A7	5,574,874
C:\Users\Criminal\Music	Bon Jovi - Livin' On A Prayer	.MP3	3EB1684FAF823A3995B4CBE7C210DAF3	5,039,165
C:\Users\Criminal\Music	Bon Jovi - It's My Life	.MP3	27B4C689719D2BF554E2268D02187794	4,493,195
C:\Users\Criminal\Music	Calvin Harris - Summer	.MP3	FD0E6722DCF61CA949A49DFC0DE6F088	8,972,320

C:\Users\Criminal\Music	C?line Dion - Because You Loved Me	.MP3	8F60B82219524D57FF3C8698DE5A7501	8,629,147
C:\Users\Criminal\Music	Foo Fighters - My Hero	.MP3	6B2F8391F1A8C3E1D1AF43607507174F	10,462,059
C:\Users\Criminal\Music	Kiss	.MP3	170DCF4410E714391531DD8939FB5D92	3,674,340
C:\Users\Criminal\Music	Lets Go Crazy	.MP3	8215FD290E4E50A752C6769C97916E55	4,560,887
C:\Users\Criminal\Music	Little Red Corvette	.MP3	23D66BF0DB8678E2E4FF436C39E39A67	4,805,346
C:\Users\Criminal\Music	Metalica - Nothing Else Matters	.MP3	982A665D1BA5E1C995AE59725DDC3B32	15,633,358
C:\Users\Criminal\Music	Metalica - Sad But True	.MP3	5B763A71D67F637CAB857C4046B33D36	13,074,387
C:\Users\Criminal\Music	Metalica - The Memory Remains	.MP3	BA042884F5A179D38E5A7EAAD4E6C2BE	11,238,723
C:\Users\Criminal\Music	Metalica - Wherever I May Roam	.MP3	D2B8D520987922D81757DD1EB6A1873E	15,689,781
C:\Users\Criminal\Music	Oh Shelia	.MP3	BD6ECC5FCE84536D5F0A7447014738D2	3,490,104
C:\Users\Criminal\Pictures	Picture21	.JPG	AF485DFF4DBEB8FA3A4A1BE6CCF359F2	15,149
C:\Users\Criminal\Pictures	Picture22	.JPG	C7584F7D11C6F47B56AFEDB7F002E299	93,053
C:\Users\Criminal\Pictures	Picture23	.JPG	85F22EB88D8D01F189AFA602E0E93997	37,281
C:\Users\Criminal\Pictures	Picture24	.JPG	2853317E41A354C53EBD396B4BB5D4D7	383,181
C:\Users\Criminal\Pictures	Picture25	.JPG	834732BEB25577665D205444D153BF58	33,330
C:\Users\Criminal\Pictures	Picture26	.JPG	90E60ABFA013487EB01980440E59D8EF	53,572
C:\Users\Criminal\Pictures	Picture27	.JPG	46CD3E7A74FA6BD39D3D7FCDC2F882B0	75,406
C:\Users\Criminal\Pictures	Picture28	.JPG	33267AE435687927CD67626ACF504FA9	128,290
C:\Users\Criminal\Pictures	Picture29	.JPG	62D51F5F88CD49C1979425DD17265B8C	51,600
C:\Users\Criminal\Pictures	Picture30	.JPG	A2833F0A2A0661D52C7DBEA90F8A387E	81,132

C:\Users\Criminal\Pictures	Picture38	.JPG	ECE7E8E15FCB1C24D605EF260008CFDB	4,790,969
C:\Users\Criminal\Pictures	Picture38	.JPG	92FDEF66E01B12EC4A65E3C3D318D80A	225,835
C:\Users\Criminal\Pictures	Picture40	.JPG	23350D7B168C595823B33DD07CF27FB0	260,449
C:\Users\Criminal\Videos	Men of Honor	.MKV	245C3A2D4AFC39C8D3FFA3AEF718DF4D	11,717,026,154
C:\Users\Criminal\Videos	Pitch Perfect 2	.MKV	CBC4F9FA89C64A4890CE4A6E3B822E3D	14,892,299,290
C:\Users\Criminal\Videos	Ted	.MKV	5C2604C79462CC8B3930A0ADEC5A2A32	8,206,955,958
C:\Users\Criminal\Videos	Top Gun	.MKV	FB20E6CB3D7FAF57A057B9CE00E586D8	10,013,372,823
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E01-E02 - London - 720p	.MP4	ABBC60A8069D684E626569FFA7C4615A	581,701,158
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E03 - The Pawnee-Eagleton Tip Off Classic - 720p	.MP4	156230644B1CFB2D8D29B38694B10000	264,390,850
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E04 - Doppelgangers - 720p	.MP4	9B65EAC2A7FB54FBCFE41F5412C482A3	271,309,757
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E05 - Gin It Up! - 720p	.MP4	73130ABDBF2197FE2B90F701D0C0C838	260,764,706
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E06 - Filibuster - 720p	.MP4	06A0E3DD07336601A70D3E46249F0273	279,415,938

C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E07 - Recall Vote - 720p	.MP4	17366F311A8E9C5F0AC11EEA07595CE5	272,130,654
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E08 - Fluoride - 720p	.MP4	3822702A0AB576DC1C91B19830886132	282,322,613
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E09 - The Cones of Dunshire - 720p	.MP4	93E111CFCFB7EB75BA34C37EEE68E672	291,291,640
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E10 - Second Chunce - 720p	.MP4	1721B6FF6AC28A10431FA462AE13FF4A	276,857,789
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E11 - New Beginnings - 720p	.MP4	65324196E5BA1594BC20B8356DC2C62D	283,561,663
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E12 - Farmers Market - 720p	.MP4	2D3154256A14F4120E3AF4D4AB78966F	302,806,644
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E13 - Ann and Chris - 720p	.MP4	FE0405A1E6E7397B1FB9E7CE4A7C6C37	287,678,055
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E14 - Anniversaries - .MP4720p	.MP4	11599EBEA97A2672AA08785BA76C1562	265,582,043

C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E15 - The Wall - 720p	.MP4	0C26180D80BDA4FD56AF5812225E3D9B	281,011,505
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E16 - New Slogan - 720p	.MP4	EE40DEAB5B5A7C0F9F306F2DA313B5B1	256,401,628
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E17 - Galentine's Day 2 - 720p	.MP4	7DA338D0B503AC6CDA100F26CEE806DD	288,031,906
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E18 - Prom - 720p	.MP4	66C7C758C67CD9A288E40587D5D6F861	296,186,292
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E19 - Flu Season 2 - 720p	.MP4	D69532C9A195D49BAE06EAF0937E90E4	279,706,618
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E20 - One in 8,000 - 720p	.MP4	1F8B475E5F78C7142F3EA4180C7ADB18	281,169,776
C:\Users\Criminal\Videos\Parks and Recreation Season 6	Parks and Recreation - S06E21-E22 - Moving Up - 720p	.MP4	49A73B0CE903E6AB0148939F9D3DADCA	640,614,857
C:\Users\Son\Desktop	PDF (36)	.PDF	CE4FE5AD8769A1707957CA446E214F8A	2,004,844
C:\Users\Son\Desktop	PDF (37)	.PDF	9DFBF8512FBE4E836A7EB5B53094C7BD	441,933
C:\Users\Son\Desktop	PDF (38)	.PDF	E7643610883F8FDA38D9682010CABE61	561,048
C:\Users\Son\Desktop	PDF (39)	.PDF	2D0B009BDE751608DC5F3B27814C750C	125,352

C:\Users\Son\Desktop	PDF (40)	.PDF	309080DE9315F3D9BD9914202EB0C609	42,047
C:\Users\Son\Desktop	Picture6	.JPG	B13A54135E9756DBFF3E208559F9F397	36,296
C:\Users\Son\Desktop	Picture7	.JPG	76F3FD8DFAD736B38D1AF3D80C5A4EE3	75,465
C:\Users\Son\Desktop	Picture8	.JPG	7F695CD00A09E1F81BA19FB937FB1725	125,048
C:\Users\Son\Desktop	Planes Fire and Rescue	.MP4	17269946C7E56C30091DE6E092B2AF15	1,328,106,823
C:\Users\Son\Documents	2014_04_msw_a4_form at	.DOC	26951EF74A3EF9816F85F65DC168E13D	57,344
C:\Users\Son\Documents	Biology Cover Letter	.DOCX	E15B33FF7E86C763B048123A5A2CBFB7	16,339
C:\Users\Son\Documents	Cover letter - Business & Management	.DOCX	918B7517C6F625CD81B36A785CB48589	17,361
C:\Users\Son\Documents	cover letter - criminal justice	.DOCX	9D77E24C86E60D61AB4233B4C26675D5	15,032
C:\Users\Son\Documents	Creating-an-Itinerary-Free-Word-Template	.DOCX	B8E258B160F79F871D80CCD6438E7A2F	392,982
C:\Users\Son\Documents	Daily-Schedule-Itineray-Template-MS-Word-Free-Download	.DOCX	F912BA28D5C7EA3B068251599E8F4221	222,159
C:\Users\Son\Documents	demo	.DOCX	B7509036448A02DBFF1F25A874A2B509	1,333,090
C:\Users\Son\Documents	easychair	.DOCX	BB79B79504CB1032CE76C3A355F4C718	2,204,407
C:\Users\Son\Documents	Event-Planning-Itinerary-Template	.DOC	7B9C86049F82D5825C9032557A807022	39,424
C:\Users\Son\Documents	Free-Download-MS-Word-Free-Itinerary-Template	.DOCX	251BF71F8C34D6A7A239013B2F4FEE21	44,200

C:\Users\Son\Documents	Free-MS-Word-Format-Travel-Itinerarry-Template	.DOC	E6C1E7C9F80918943029A2FCB99F855C	539,648
C:\Users\Son\Documents	Free-Word-Kick-off-Planning-Itineraray-Template	.DOCX	8CFAFBA63325439AAA36455A8080260F	107,266
C:\Users\Son\Documents	Georgia_opposition_NATO-Eng-F	.DOC	A934B321295DC1BAFE2BE3BA2F616B7C	34,816
C:\Users\Son\Documents	Georgij Lesnikov - CV	.DOC	F08934C6DF1CED750E345C24663F9C51	67,584
C:\Users\Son\Documents	imrtemplate	.DOCX	4CFC49E973F2E124FC9A4256B1DAB45F	35,947
C:\Users\Son\Documents	mastersinstructions	.DOC	904FDF0C702A1E6A320B9E1511505227	218,112
C:\Users\Son\Documents	MS-Word-2010-Format-Wedding-Itinerary-Template	.DOC	4A166A47BC0A3B6E4460088F77D9BB23	28,672
C:\Users\Son\Documents	PDF (21)	.PDF	232A3F09AC6662BB944434156A488147	2,817,749
C:\Users\Son\Documents	PDF (22)	.PDF	649BFF6038F1DC3A421FAD60E2AEE834	448,583
C:\Users\Son\Documents	PDF (23)	.PDF	6FCE936F1687DC7481E27D95EC63DE0F	30,963,393
C:\Users\Son\Documents	PDF (24)	.PDF	03AC2D82C0EC034BB46DAB3AA13F3E07	1,872,709
C:\Users\Son\Documents	PDF (25)	.PDF	C10187B5680E5B5DB91E2EC0A1485FE5	262,234
C:\Users\Son\Documents	PDF (26)	.PDF	3C62B475903CC8F37278438149E6A046	397,654
C:\Users\Son\Documents	PDF (27)	.PDF	567D99BEBAC52C43C8C7EDED17DA8CFA	6,782,631
C:\Users\Son\Documents	PDF (28)	.PDF	E2DC57B9DB873EF3AD7CB9D29F3BE698	642,486
C:\Users\Son\Documents	PDF (29	.PDF	DC111D8ED66F400B3C0B917DBA011BEE	443,604
C:\Users\Son\Documents	PDF (30)	.PDF	98A56D2AABF0D4FC34D8445F0CE6F4AD	410,991

C:\Users\Son\Documents	PDF (31)	.PDF	769A1A43A7C4C9AC8C25FE27C74D0E99	82,187
C:\Users\Son\Documents	PDF (32)	.PDF	B8C50F725598479D355438C633C595EC	961,152
C:\Users\Son\Documents	PDF (33)	.PDF	ED94016BD46025D58AC8087211BBFA16	84,002
C:\Users\Son\Documents	PDF (34)	.PDF	2C313A108912AAD1FF3D4B11B8EF90E1	315,488
C:\Users\Son\Documents	PDF (35)	.PDF	10F6F97E3A4C2F638F422FCBD9275E21	429,366
C:\Users\Son\Documents	Picture12	.JPG	D76EAC902FC1F1EDAFAE8E96995502C7	13,153,160
C:\Users\Son\Documents	Picture13	.JPG	A64280C516588130C8FD0BDCE06D7443	5,482,981
C:\Users\Son\Documents	Picture14	.JPG	2F9D6ACC608BB6C948667E3643404586	6,479,629
C:\Users\Son\Documents	Picture15	.JPG	08F78220547BC5AC56439F56FA4CACDF	6,956,283
C:\Users\Son\Documents	Picture16	.JPG	F977F913F9B7232BFEDE6EE5601C005B	1,059,406
C:\Users\Son\Documents	Picture17	.JPG	126A26619A30226CD90691B04D06D569	208,836
C:\Users\Son\Documents	Picture9	.JPG	B35075835732ACD6EB31F58619134108	188,303
C:\Users\Son\Documents	SampleDOCFile_100kb	.DOC	4198FB827362BBB68A72498100B5D7BD	102,400
C:\Users\Son\Documents	SampleDOCFile_200kb	.DOC	4BE15CC6978DE204946CB161C3D18AA9	204,288
C:\Users\Son\Documents	SampleDOCFile_500kb	.DOC	8E98658AEE1D90B81B313C90A3BC161F	512,000
C:\Users\Son\Downloads	Picture10	.JPG	EE4A5C0132FC1477F4D099F9D840F50D	71,106
C:\Users\Son\Downloads	Picture11	.JPG	D1974CAB58A9AA7C338BE6342D7A1684	4,920,723
C:\Users\Son\Music	01 Don't Stop Til You Get Enough	.MP3	B61BFC4422EC506B559DA4A99E3162AA	3,798,643
C:\Users\Son\Music	01 Life Is a Highway	.MP3	E2FBC53814E95DC99E75E8E1CBC1B4F2	6,654,597
C:\Users\Son\Music	02 Rock With You	.MP3	DCBE33971D49BE299A7955763809E332	3,553,379
C:\Users\Son\Music	03 Billie Jean	.MP3	C2F5D8D82BFC73306A5703F398C370F8	4,713,105
C:\Users\Son\Music	03 Let's Stay Together	.MP3	C9B9454EB717BE87323A5776D3483EB3	8,051,495
C:\Users\Son\Music	04 Beat It	.MP3	D22AC0D5FFF1F948340C6EE5627D78E9	4,152,653

C:\Users\Son\Music	05 Thriller	.MP3	DF2AECEF713C49456EC63D64A91A3A24	5,003,745
C:\Users\Son\Music	08 Can I Take You Out Tonight	.MP3	1E7BB14D2EDC139704D48A97C9D3D8ED	5,484,224
C:\Users\Son\Music	11 Bless The Broken Road	.MP3	40835D5282272E68389D2588DB02078A	4,683,332
C:\Users\Son\Music	11 Wagon Wheel	.M4A	8EA26C046FC44EB37C92DB37717E0CB3	7,653,866
C:\Users\Son\Music	Good Morning Beautiful	.MP3	67420E56058DE68276D679ECC09FD8FB	3,417,901
C:\Users\Son\Music	Hot Blooded	.MP3	7705AE88AD643D0419020A2E5B5A2DEA	4,227,512
C:\Users\Son\Music	I'm Moving On	.MP3	4E4D88833AAEF49209B454C7E6CF7E1D	3,920,309
C:\Users\Son\Music	Purple Rain	.MP3	5D1F2B2BA4C7DC7FECC56D834CB50621	8,391,532
C:\Users\Son\Music	Raspberry Beret	.MP3	D86D285912EB94EC65CF8F29D6901EEF	5,127,099
C:\Users\Son\Music	REO Speedwagon - Can't Fight This Feeling	.MP3	B2E9DD78AA9195BAFC94CBE494603044	11,931,898
C:\Users\Son\Music	REO Speedwagon - Keep on Loving You	.MP3	495F463AFDDB2E708C446FF5E787F294	8,302,778
C:\Users\Son\Music	Royals (Lorde Cover)	.MP3	B48D2861A949945B1ACE756602491C24	4,394,675
C:\Users\Son\Music	Shawn Mendes - Mercy	.MP3	B68FF817BC22EACC5A7F51B89258709D	8,551,484
C:\Users\Son\Music	When Doves Cry	.MP3	07AC62F4BDA130DA63B6A44148C63BDB	5,021,057
C:\Users\Son\Pictures	Picture1	.JPG	F243273AD06A2CBD364A4DBCB2952C37	43,083
C:\Users\Son\Pictures	Picture18	.JPG	E964E2F1E586F7218A379D232064D078	4,246,360
C:\Users\Son\Pictures	Picture19	.JPG	A5E8CD2F4034E18CBD96DACB2026B9E7	11,294,874
C:\Users\Son\Pictures	Picture2	.JPG	2FC453DA4CE077F7E267627FBC780D93	61,079
C:\Users\Son\Pictures	Picture20	.JPG	DFD793866107345F28C260A7BEBB30F5	100,710

C:\Users\Son\Pictures	Picture3	.JPG	B1A1C8B2FA705DDA31AF2797FB137F73	84,627
C:\Users\Son\Pictures	Picture4	.JPG	C3FA51424D509C245528C5AF1920A5E0	55,397
C:\Users\Son\Pictures	Picture5	.JPG	409623732172EED6F06072CA2219C19B	269,776
C:\Users\Son\Videos	2017 Solar Eclipse	.MP4	4F4DD3BEA187FEA05250CCD77C2D190E	10,204,034
C:\Users\Son\Videos	250,000 Dominoes - The Incredible Science Machine GAME ON!	.MP4	2F0819100349541B2757876A718E029F	78,833,749
C:\Users\Son\Videos	3 Weird Alarm Clocks Never Buy This	.MP4	AB208BED4EBB11101E19E0E8F3D76346	56,876,233
C:\Users\Son\Videos	CASH or TRASH 10 Strange Chinese Items!	.MP4	49D8902C4D1DDE438DD2646103F54FD4	90,763,861
C:\Users\Son\Videos	How To Make A FIDGET SPINNER Out Of CAKE It Actually SPINS! Yolanda Gampp How To Cake It	.MP4	EB55D662E36BAD679777F7C77825C4BB	240,684,926
C:\Users\Son\Videos	Law & Order Special Victims Unit - S14E14 - Secrets Exhumed - 480p	.MP4	33071F4A34065389C81FB12F5340F7B7	220,319,571
C:\Users\Son\Videos	Law & Order Special Victims Unit - S14E16 - Funny Valentine - 480p	.MP4	D3F41CAF77F18112CFA4770B9D71309F	266,783,650

C:\Users\Son\Videos	Law & Order Special Victims Unit - S14E18 - Legitimate Rape - 480p	.MP4	FE2F1D1E69B3B61325E195CC6138F05F	242,532,520
C:\Users\Son\Videos	Law & Order Special Victims Unit - S14E23 - Brief Interlude - 480p	.MP4	3BDA37BB0E889CB35F94B964828EE4C9	267,961,010
C:\Users\Son\Videos	Law & Order Special Victims Unit - S15E06 - October Surprise - 480p	.MP4	0BD2706BB4EA430270B813E83D053B13	249,887,303
C:\Users\Son\Videos	Law & Order Special Victims Unit - S15E07 - Dissonant Voices - 480p	.MP4	727D397DBC83C6FDB474E939ED83BB94	251,713,017
C:\Users\Son\Videos	Law & Order Special Victims Unit - S15E13 - Betrayal's Climax - 480p	.MP4	900B1BD01B764EC390B7EBC04C81BD1B	261,991,282
C:\Users\Son\Videos	Law & Order Special Victims Unit - S16E18 - Devastating Story - 480p	.MP4	7454A6B5592EBBC3AE54496176A85AB9	297,222,843

C:\Users\Son\Videos	Light Balance Glowing Dance Crew Illuminates the AGT Stage - America's Got Talent 2017	.MP4	A377FDD2C29562AE755A470E901A3385	9,523,265
C:\Users\Son\Videos	World Record Edition Dude Perfect	.MP4	48BC61D39915DB69B519D8A0A67D9DF1	44,076,694
C:\Users\Son\Videos	You Will Laugh Till You FART - World's FUNNIEST Compilation	.MP4	EFDAC3A86FC3679815F7D56A3029A660	115,611,689
C:\Users\Son\Videos\The Dark Knight Trilogy	Batman Begins	.MKV	F4752A55ED0AFE744996ED33A5BDABBF	17,298,012,145
C:\Users\Son\Videos\The Dark Knight Trilogy	The Dark Knight Rises	.MKV	878BCF0AFC769DA37282066842A042EF	22,901,816,449
C:\Users\Son\Videos\The Dark Knight Trilogy	The Dark Knight	.MKV	BA5EDB6BB96793EE2CE7956B8F004B29	18,488,834,169

APPENDIX B: ACQUSITION RESULTS

FTK Imager Live Acquisition Results

Name	Start Time	End Time	MD5 Hash Value	Total Time (sec)	Total Size (MBs)	Total Speed (MB/s)
FTK_Imager_Live.001	11:18:42	11:57:38	ef63c355c3e05ac4ec447315ee37544f	2,336	244,191	104.53
FTK_Imager_Live2.001	14:14:39	14:57:48	338f9cc45eb69ca9cfd8139ee54ad7a2	2,589	244,191	94.32
FTK_Imager_Live3.001	6:42:01	7:44:54	7cd41c1b8280b06a525020158bad2ab0	3,773	244,191	64.72
FTK_Imager_Live4.001	10:01:57	10:41:03	22174acc79ffc7b4a0f04e025fd71e7e	2,346	244,191	104.09
FTK_Imager_Live5.001	11:21:14	12:04:54	7d820966ce4ac7ce30a45555f534b367	2,620	244,191	93.20
FTK_Imager_Live6.001	15:55:29	16:58:15	1498aac5be1cc9e3a25ebec3f829bd9b	3,766	244,191	64.84
FTK_Imager_Live7.001	18:08:54	18:47:59	5927320a64b533b778663b2de25b4516	2,345	244,191	104.13
FTK_Imager_Live8.001	19:27:23	20:10:56	bb9c8c7f8c6fa0406ccb4dc1bd9b8ae6	2,613	244,191	93.45
FTK_Imager_Live9.001	4:24:47	5:27:39	c69cb682c3862a894e2abb3e7174b3fa	3,772	244,191	64.74
FTK_Imager_Live10.001	8:17:01	8:56:04	923028bdd5ed1ebf29e45aa6bcb443be	2,343	244,191	104.22
Averages				**2,850**	**244,191**	**89.22**

FTK Imager Dead Acquisition Results

Name	Start Time	End Time	MD5 Hash Value	Total Time (sec)	Total Size (MBs)	Total Speed (MB/s)
FTK_Imager_Dead1.e01	7:25:01	8:17:39	d1101102219d5dae5f01da2391e00e6c	3,158	243,631	77.15
FTK_Imager_Dead2.e01	8:17:39	9:10:12	d1101102219d5dae5f01da2391e00e6c	3,153	243,631	77.27
FTK_Imager_Dead3.e01	9:10:12	10:02:50	d1101102219d5dae5f01da2391e00e6c	3,158	243,631	77.15
FTK_Imager_Dead4.e01	10:02:50	10:55:57	d1101102219d5dae5f01da2391e00e6c	3,187	243,631	76.45
FTK_Imager_Dead5.e01	10:55:57	11:49:01	d1101102219d5dae5f01da2391e00e6c	3,184	243,631	76.52
FTK_Imager_Dead6.e01	11:49:01	12:42:14	d1101102219d5dae5f01da2391e00e6c	3,193	243,631	76.30
FTK_Imager_Dead7.e01	12:42:14	13:36:40	d1101102219d5dae5f01da2391e00e6c	3,266	243,631	74.60
FTK_Imager_Dead8.e01	13:36:40	14:30:02	d1101102219d5dae5f01da2391e00e6c	3,202	243,631	76.09
FTK_Imager_Dead9.e01	14:30:02	15:23:29	d1101102219d5dae5f01da2391e00e6c	3,207	243,631	75.97
FTK_Imager_Dead10.e01	15:23:29	16:17:05	d1101102219d5dae5f01da2391e00e6c	3,216	243,631	75.76
Averages				**3,192**	**243,631**	**76.32**

DD Command Live Acquisition Results

Name	Start Time	End Time	MD5 Hash Value	Total Time (sec)	Total Size (MBs)	Total Speed (MB/s)
DD_Live_Image.dd	8:07:12	12:22:06	488b51198be45e65d9831d80567c0eed	15,294	265,060	16.74
DD_Live_Image2.dd	12:27:06	16:42:22	0d41a8f6687f311883660d25dB69b5ab	15,316	265,060	16.72
DD_Live_Image3.dd	16:47:22	21:03:21	3163bc05203fec74639455e3398cd938	15,359	265,060	16.67
DD_Live_Image4.dd	21:08:21	1:24:42	371cf2e7a7a6c3201413570db68b025d	15,381	265,060	16.65
DD_Live_Image5.dd	1:29:42	5:46:08	4e3946d293730d130498561def03c8fd	15,386	265,060	16.64
DD_Live_Image6.dd	5:51:08	10:06:54	6789eb905c4b94149e0fe5a00f0669ac	15,346	265,060	16.69
DD_Live_Image7.dd	10:11:54	14:27:04	3b8cbc6c765e26847eeacae15a0956c9	15,310	265,060	16.73
DD_Live_Image8.dd	14:32:04	18:48:09	3852442b0d18d21dec1129bdf61cd259	15,365	265,060	16.67
DD_Live_Image9.dd	18:53.09	23:07:53	ba7093e38556ac1c4e8695e855ab213b	15,284	265,060	16.75
DD_Live_Image10.dd	23:12:53	3:28:04	badf767e4e07b3aa30519ee6d67d7176	15,311	265,060	16.72
Averages				**15,335**	**265,060**	**16.70**

DD Command Dead Acquisition Results

Name	Start Time	End Time	MD5 Hash Value	Total Time (sec)	Total Size (MBs)	Total Speed (MB/s)
DD_Dead_Image.dd	16:02:22	16:27:56	d1101102219d5dae5f01da2391e00e6c	1,534	255,465	166.54
DD_Dead_Image2.dd	16:27:56	16:49:49	d1101102219d5dae5f01da2391e00e6c	1,313	255,465	194.57
DD_Dead_Image3.dd	16:49:49	17:12:00	d1101102219d5dae5f01da2391e00e6c	1,331	255,465	191.93
DD_Dead_Image4.dd	17:12:00	17:34:29	d1101102219d5dae5f01da2391e00e6c	1,329	255,465	189.37
DD_Dead_Image5.dd	17:34:29	17:54:09	d1101102219d5dae5f01da2391e00e6c	1,360	255,465	187.84
DD_Dead_Image6.dd	17:57:09	18:20:08	d1101102219d5dae5f01da2391e00e6c	1,379	255,465	185.25
DD_Dead_Image7.dd	18:20:08	18:43:23	d1101102219d5dae5f01da2391e00e6c	1,395	255,465	183.13
DD_Dead_Image8.dd	18:43:23	19:06:56	d1101102219d5dae5f01da2391e00e6c	1,413	255,465	180/80
DD_Dead_Image9.dd	19:06:56	19:30:48	d1101102219d5dae5f01da2391e00e6c	1,432	255,465	178.40
DD_Dead_Image10.dd	19:30:48	19:54:29	d1101102219d5dae5f01da2391e00e6c	1,451	255,465	176.06
Averages				**1,396**	**255,465**	**183.39**

Paladin Dead Acquisition Results

Name	Start Time	End Time	MD5 Hash Value	Total Time (sec)	Total Size (MBs)	Total Speed (MB/s)
Paldin_Dead_Image.e01	21:41:05	23:23:55	d1101102219d5dae5f01da2391e00e6c	6,170	255,465	41.40
Paldin_Dead_Image2.e01	23:27:05	1:04:02	d1101102219d5dae5f01da2391e00e6c	5,817	255,465	43.92
Paldin_Dead_Image3.e01	5:17:20	6:57:25	d1101102219d5dae5f01da2391e00e6c	6,005	255,465	42.54
Paldin_Dead_Image4.e01	6:58:57	8:40:16	d1101102219d5dae5f01da2391e00e6c	6,079	255,465	42.02
Paldin_Dead_Image5.e01	16:05:09	17:39:38	d1101102219d5dae5f01da2391e00e6c	5,669	255,465	45.06
Paldin_Dead_Image6.e01	17:43:20	19:22:35	d1101102219d5dae5f01da2391e00e6c	5,955	255,465	42.90
Paldin_Dead_Image7.e01	19:31:06	21:07:18	d1101102219d5dae5f01da2391e00e6c	5,772	255,465	44.26
Paldin_Dead_Image8.e01	22:55:14	0:30:59	d1101102219d5dae5f01da2391e00e6c	5,745	255,465	44.47
Paldin_Dead_Image9.e01	2:08:00	3:39:41	d1101102219d5dae5f01da2391e00e6c	5,501	255,465	46.44
Paldin_Dead_Image10.e01	7:21:21	8:55:11	d1101102219d5dae5f01da2391e00e6c	5,630	255,465	45.38
Averages				**5,834**	**255,465**	**43.84**

Paladin Dead DD Acquisition Results

Name	Start Time	End Time	MD5 Hash Value	Total Time (sec)	Total Size (MBs)	Total Speed (MB/s)
Paldin_Dead_Image.dd	14:27:27	14:56:51	d1101102219d5dae5f01da2391e00e6c	1,764	255,465	144.82
Paladin_Dead_Image2.dd	15:26:44	15:56:52	d1101102219d5dae5f01da2391e00e6c	1,808	255,465	141.30
Paladin_Dead_Image3.dd	16:09:18	16:40:15	d1101102219d5dae5f01da2391e00e6c	1,857	255,465	137.57
Paladin_Dead_Image4.dd	17:20:33	17:52:25	d1101102219d5dae5f01da2391e00e6c	1,912	255,465	133.61
Paladin_Dead_Image5.dd	17:53:04	18:25:55	d1101102219d5dae5f01da2391e00e6c	1,971	255,465	129.61
Paladin_Dead_Image6.dd	18:49:25	19:23:31	d1101102219d5dae5f01da2391e00e6c	2,046	255,465	124.86
Paladin_Dead_Image7.dd	19:24:33	19:59:44	d1101102219d5dae5f01da2391e00e6c	2,111	255,465	121.02
Paladin_Dead_Image8.dd	20:00:54	20:37:47	d1101102219d5dae5f01da2391e00e6c	2,213	255,465	115.44
Paladin_Dead_Image9.dd	20:38:37	21:17:20	d1101102219d5dae5f01da2391e00e6c	2,323	255,465	109.97
Paladin_Dead_Image10.dd	21:28:29	22:09:18	d1101102219d5dae5f01da2391e00e6c	2,449	255,465	104.31
Averages				**2,045**	**255,465**	**126.25**

REFERENCES

Al-Fedaghi, S., & Al-Babtain, B. (2012). Modeling the forensics process. *International Journal of Security and Its Applications*, *6*(4), 97–108.

Årnes, A. (2017). *Digital Forensics*. Hoboken, NJ: John Wiley & Sons.

Arthur, W., Challener, D., & Goldman, K. (2015). *A Practical Guide to TPM 2.0*. https://doi.org/10.1007/s13398-014-0173-7.2

Bell, G., & Boddington, R. (2010). Solid state drives: the beginning of the end for current practice in digital forensic recovery? *The Journal of Digital Forensics, Security and Law*, *5*(3), 5–32.

Benusa, A. D., Jeganathan, S. S., & Schmidt, M. B. (2016). Shift from HDD to SSD storage present forensic analysis challenges. In *Information Institute Conferences* (pp. 1–17). Las Vegas, NV.

Bone, B. (AccessData). (2016). Run FTK imager from a flash drive (Imager Lite). Retrieved March 1, 2017, from https://support.accessdata.com/hc/en-us/articles/203681809-Run-FTK-Imager-from-a-flash-drive-Imager-Lite-

Bonomo, R., Dayan, R. A., Freeman, J. W., Johnson, R. D., Nolterieke, D., & Springfield, R. S. (2003). Method, system, and program for customizing a basic input/output system ("BIOS") configuration according to the type of user.

Brian Carrier. (2005). *File system forensic analysis*. *Computer*. Addison Wesley Professional. https://doi.org/10.1016/B978-1-59749-472-4.00002-0

Carnegie Mellon University. (2017). How cyber criminals operate. Retrieved January 1, 2017, from http://www.carnegiecyberacademy.com/facultyPages/cyberCriminals/catching.html

Carrier, B. (2017). The Sleuth Kit. Retrieved from https://www.sleuthkit.org/about.php

Casey, E. (2011). *Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet* (Third). Baltimore, MD: Elsevier Inc.

Casey, E., & Schatz, B. (2011). Conducting digital investigations. In *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd Edition*.

Department of Homeland Security. (2016). *FTK Imager v3.4.2.6*. Retrieved from https://www.dhs.gov/sites/default/files/publications/1491_508_Test Report_NIST_Disk Imaging_FTK Imager v3.4.2.6_October_14_2016.pdf

Department of Homeland Security, & United States Secret Service. (2007). *Best Practices - For Seizing Electronic Evidence v3. United States*. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=12704545&site=ehost-live

Easttom, C. (2014). *System Forensics, Investigation, and Response* (2nd ed.). Burlington: Jones & Bartlett Learning, LLC.

Garfinkel, S. L. (2007). Carving contiguous and fragmented files with fast object validation. *Digital Investigation*, *4*(SUPPL.), 2–12. https://doi.org/10.1016/j.diin.2007.06.017

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*(SUPPL.). https://doi.org/10.1016/j.diin.2010.05.009

Gohel, H., & Upadhyay, H. (2017). Cyber threat analysis with memory forensics. *CSI Communications*, *40*(11), 17–19.

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the U.S. criminal justice system. *Priority Criminal Justice Needs Initiative*, 1–32. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

Grobler, T., Louwrens, C. P., & Solms, S. H. von. (2010a). A Multi-component view of digital forensics. In *RES 2010 - 5th International Conference on Availability, Reliability, and Security*. (pp. 647–652). https://doi.org/10.1109/ARES.2010.61

Grobler, T., Louwrens, C. P., & Solms, S. H. von. (2010b). A Multi-component View of Digital Forensics. In *RES 2010 - 5th International Conference on Availability, Reliability, and Security*. (pp. 647–652). https://doi.org/10.1109/ARES.2010.61

Intel Corporation. (2012). What Is An Ultrabook Device. Retrieved December 11, 2017, from https://software.intel.com/sites/default/files/WhatIsUltrabook.pdf

Judish, N., Hagen, E., Bailie, M., & Jarrett, H. (2009). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Office of Legal Education. Retrieved from https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

Kemmerich, T., Junge, F., Kuntze, N., Rudolph, C., Endicott-Popovsky, B., & Grosskopf, L. (2014). Generation and handling of hard drive duplicates as piece of evidence. In *ADFSL Conference on Digital Forensics, Security and Law* (pp. 73–82).

Kornblum, J. (2006). Identifying almost identical files using context triggered piecewise hashing. *Digital Investigation*, *3*(SUPPL.), 91–97. https://doi.org/10.1016/j.diin.2006.06.015

Kumar, S., & Vijayaraghavan, R. (2015). Solid State Drive (SSD), *37*(210), 2552–2553. Retrieved from https://pdfs.semanticscholar.org/a8a8/8562ebd9abc027d2d28023991cec0edc2252.pdf

Lyle, J. R. (2006). A strategy for testing hardware write block devices. *Digital Investigation*, *3*(SUPPL.), 3–9. https://doi.org/10.1016/j.diin.2006.06.001

Mckemmish, R. (2008). When is digital evidence forensically sound? In *Advances in Digital Forensics IV* (pp. 3–15).

Menz, M., & Bress, S. (2004). The fallacy of software write protection in computer forensics. *Technology*. Retrieved from http://mykeytech.com/softwarewriteblocking2-4.pdf

Merrian-Webster. (2017a). Gigabyte. Retrieved September 11, 2017, from https://www.merriam-webster.com

Merrian-Webster. (2017b). Terabyte. Retrieved September 11, 2017, from https://www.meriam-webster.com

Micheloni, R., Marelli, A., & Eshghi, K. (2013). *Inside Solid State Drives (SSDs)*. Springer.

Movall, P., Nelson, W., & Wetzstein, S. (2005). Linux Physical Memory Analysis. *USENIX*. Retrieved from http://static.usenix.org/publications/library/proceedings/usenix05/tech/freenix/full_papers/movall/movall_html/

NIST. (2003). Software Write Block Tool Specification & Test Plan.

NIST. (2004). Hardware Write Blocker Device (HWB) Specification.

NIST. (2017). Disk Imaging. Retrieved from https://www.cftt.nist.gov/disk_imaging.htm

Paulsen, J. (2016). Designing efficient storage systems. In *Flash Memory Summit*. Retrieved from http://blog.seagate.com/intelligent/keynote-designing-efficient-storage-systems-using-both-flash-and-hdds/

Pollitt, M. (2010). A history of digital forensics. In K.-P. Chow & S. Shenoi (Eds.), *Advances in Digital Forensics VI* (Vol. 337, pp. 3–15). Hong Kong, China: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-15506-2

Rivest, R. (1992). The MD5 message-digest algorithm. *IETF RFC 1321*, 1–21. Retrieved from https://tools.ietf.org/pdf/rfc1321.pdf

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law*, *1*(2), 19–38. https://doi.org/10.1.1.169.1878

Seagate. (2017). Barracuda. Retrieved from https://www.seagate.com/www-content/product-content/barracuda-fam/barracuda-new/files/barracuda-2-5-ds1907-1-1609us.pdf

Shabana Subair, P., Balan, C., Dija, S., & Thomas, K. L. (2014). Forensic decryption of FAT BitLocker volumes. *Digital Forensics and Cyber Crime: Fifth International Conference, ICDF2C 2013 Moscow, Russia, September 26-27, 2013 Revised Selected Papers*, *132*, 17–29. https://doi.org/10.1007/978-3-319-14289-0

Shim, R. (2012). Tablets impact the notebook market: Enter the ultrabook. *Information Display*, *28*(2–3), 12–14.

St.Amant, K., & Still, B. (2007). *Handbook of Research on Open Source Software: Technological, Economic, and Social Perspectives*. *Handbook of Research*. Hershey: Information Science Reference. https://doi.org/10.1109/TPC.2008.2007877

SWGDE. (2013). Best Practices for Mobile Phone Forensics, *0*, 1–12. Retrieved from https://www.swgde.org/documents/Current Documents/2013-02-11 SWGDE Best Practices for Mobile Phone Forensics V2-0

SWGDE. (2014). Best Practices for Computer Forensics. *Scientific Working Group on Digital Evidence*, *1*, 1–12.

SWGDE. (2014). Capture of Live Systems. *Scientific Working Group on Digital Evidence*, *1*, 1–6.

Tableau. (2017). T35u & T35u-RW quick reference guide. Guidance Software. Retrieved from https://www.guidancesoftware.com/docs/default-source/document-library/quick-start-guide/t35u-quick-reference-guide.pdf?sfvrsn=c6218bad_12

Tahiri, S. (2016). Digital Forensics Models. Retrieved January 1, 2017, from http://resources.infosecinstitute.com/digital-forensics-models/

Vamsee, K. (2011). Solid state drive vs. hard disk drive: Price and performance study. *Dell PowerVault Storage System*, 1–13. Retrieved from http://www.dell.com/downloads/global/products/pvaul/en/ssd_vs_hdd_price_and_performance_study.pdf

Vandeven, S. (2014). Forensic images: For your viewing pleasure. *SANS Institute InfoSec Reading Room*. Retrieved from https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447

Waring, J. (2014). Number of devices to hit 4.3 per person by 2020 - report. Retrieved March 4, 2017, from http://www.mobileworldlive.com/featured-content/home-banner/connected-devices-to-hit-4-3-per-person-by-2020-report/

Western Digital. (2017). WD Gold Enterprise-class Hard Drives. Retrieved from http://products.wdc.com/library/SpecSheet/ENG/2879-800074.pdf